empirica

Benchmarking in a Policy Perspective

Report No. 8

Security and confidence

November 2007

Disclaimer

The views expressed in this draft report are those of the authors and do not necessarily reflect those of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the information provided in this document.

The data used for the present report comes from the Eurostat Community Surveys on ICT Usage and e-Commerce in Enterprises 2003-2006 and has been provided by Eurostat. No further data quality and consistency checks have been carried out by the authors; the data was used as provided by Eurostat and the European Commission.

Contact

This report was elaborated by:

empirica

Gesellschaft für Kommunikations-
und Technologieforschung mbH

Oxfordstr. 2, D-53111 Bonn

Germany

Tel.: +49 (0)228 98 539 0
Fax: +49-(0) 228 98530-12

info@empirica.com

Rights Restrictions

Bonn and Brussels, November 2007

Table of contents

Index of tables

Tables

1 Introduction to the Project “Benchmarking in a Policy Perspective”

1.1 Objectives

The project “Benchmarking in a Policy Perspective” was started by the European Commission in January 2006.

The objective of the “Benchmarking in a Policy Perspective” project initiated by the European Commission is to carry out an in-depth analysis of the results of the annual Information Society Surveys of households and enterprises and to relate them to a number of specific themes. The aim is to address areas beyond simple ICT connectivity and highlight intensity of use and wider impact on individuals, enterprises and communities.

1.2 Expected Outcomes

The project develops Topic Reports for which an in-depth analysis of available survey results is carried out. Up to now the following reports have been produced. A further report will feature a summary of key findings and will be delivered at the end of the project.

Table 1-1 Topic Reports produced by the project “Benchmarking in a Policy Perspective

No.	Topic	Date
1	e-Business and the reorganisation of business processes	March 2006
2	Use of broadband	May 2006
3	Take up of advanced services	July 2006
4	Use of public services on line (including eGovernment and eHealth)	September 2006
5	Inclusion	November 2006
6	Digital literacy and ICT Skills	April 2007
7	Recommendations for two questionnaire modules on e-commerce and trust	June 2007
8	Security	December 2007

Most topic reports have so far covered the following items:

- Review of the basic concept and policy issues related to the theme,
- An analysis of past and current Community survey results to provide an overview of progress in the EU,
- A comparison with existing empirical evidence on the same issue to assess the robustness of the results and provide additional qualitative analysis,
- An investigation of international sources to compare EU achievements with its main competitors,
- A proposal for re-wording or expanding the questionnaire used by EUROSTAT for future surveys.

2 Objective

E-security is likely to become a key factor in the Information Society as the use of ICT plays a increasingly large role in economic and social life. There are various issues arising from the development of network and information systems and corresponding security needs.

Security is a dynamic issue as the speed of technological development increases – leading to new types of threats on the one hand and new security solutions (products and applications) on the other hand. Especially after the 11th of September 2001 an increased awareness of general security issues also gave e-security bigger importance, since the Internet can in principle become the object of terrorist attacks or a medium for preparing and carrying out attacks.

Additionally, changes in the ICT environment result in the need for new security solutions: More and more sensitive data and economically viable information is processed; "always-on" connections and wireless local area networks are spreading fast.

The objective of this document is to review existing surveys, both of households and enterprises, addressing the issue of security and confidence and to collate them in a thematically structured way.

Preliminary Note:

In January 2008, shortly after the editorial deadline of this report the European Network and Information Security Agency ENISA has released a report named **"Examining the feasibility of a data collection framework"**.

This report among other things reports about various existing data collection initiatives, surveys and reports. It builds upon two years work and a network of stakeholders and therefore its comprehensiveness as regards international data sources goes significantly beyond the scope of this report. The interested reader is recommended to also consult this report and the sources linked therein for a complete overview of data sources.

3 Experience with previous security indicators

Three quotes from relevant Commission documents sum up the current situation and satisfaction of the statistical community with the security statistics practice to date:

In the document "Results of the survey on the relevance of indicators for benchmarking i2010, conducted among statisticians and policy makers, July 2005" (Doc.F6/ISS-WG/Oct 05/02 (original)) which was handed out in the to the Information Society Statistics (ISS) Working Group at their meeting in Luxembourg, 6 - 7 October 2005, it is acknowledged that

> *"One remarkable result of this survey is that all ICT-security indicators scored a negative result. While the area is, no doubt, of high relevance for Information Society, the previous eEurope 2005 benchmarking indicators showed several feasibility problems and the new ones proposed don't seem to answer to policy makers needs."*

The i2010 High Level Group concedes in their Benchmarking Framework:

> *"…the current questions (and the existing indicators) have proved to be inadequate – especially in the household survey: respondents do not have the technical knowledge to understand the concepts used or simply don't know whether their devices are protected and/or had a recent update*

and that

> *"For businesses, the indicators on the percentage of enterprises having encountered security problems and the percentage of enterprises that have updated security devices have proved not to be reliable. Only the indicator on enterprises taking ICT security precautions proved to be feasible. "*

The reported difficulties are amazing, when looking at the survey questions in detail. It is not clear why respondents feel such a difficulty in answering questions about whether their computer has a virus checking program or a firewall installed. One might conclude that respondents who are overstrained by such questions will be very unlikely to have the security precautions in place and then accept that imply that such a hypothesis informs the actual statistical product. However this might be a too far reaching assumption for the statistical accuracy the user expects of official statistics data.

However, it has to be accepted that for the time being, these questions overstrain respondents. Since this is not a satisfactory basis on which to draw up recommendation for measurement, we therefore want to have our recommendations be understood as a preliminary choice, deserving further investigation.

Therefore, the focus of this report lies in primarily listing existing indicators. More needs to be understood about the inabilities of respondents to provide information about their security behaviour first, before feasibility can be assessed.

Hypotheses regarding the feasibility problems of the Eurostat questionnaire include

For household surveys

- lack of expertise with the technical terms such as virus, firewall etc.
- inability to trace back any incident to a certain cause (virus / adware / spyware / fraud)
- ambiguous or vague question wording (e.g. asking respondents to assess a website's level of security ("lack of security of payments") when they can not possibly overlook all potential risks)

For enterprise surveys

- for SMEs: lack of expertise with the technical terms
- outsourcing of security to specialist, therefore inability to know technical details
- reluctance to admit problem in their own IT systems

4 Existing surveys and guidelines

4.1 Household surveys

Existing indicators are presented broken down by the following categories

- Security awareness and barriers
- Security incidents and its cost and impact
- Security behaviour

4.1.1 Security awareness and barriers

With regard to security awareness and barriers Eurostat has surveyed mainly respondents' barriers to using or accessing the internet or services in the past surveys. In most cases, non-users were asked about the reasons for not using or having access, and among the list of potential causes, security concerns were listed. This has applied to having home internet access, buying online, e-government and "more intensive internet use".

This kind of question hence mostly implicitly assumes that there are no security related barriers among those who use a service. However, this is not necessarily the case. Users may of course trust one service and not trust another.

Understanding the awareness of people using the internet, the OECD survey suggests some indicators which give an insight to negative experience of people using the internet. By this experience people lose trust in using modern technologies, especially if they don’t know how they can protect their data in the future.

Table 4-1 Overview of existing household indicators of security awareness and barriers

Security awareness and barriers indicators	Source
Security concerns as barrier to home internet access	ESTAT
Security concerns as barrier to buying online	ESTAT
Privacy concerns as barrier to buying online	ESTAT
Trust concerns as barrier to buying online	ESTAT
Complaint / redress concerns as barrier to buying online	ESTAT
Security concerns as barrier to e-government	ESTAT
Security concerns as barrier to more intensive internet use	ESTAT

See Annex for full description of the indicators

4.1.2 Security incidents and its cost and impact

Eurostat has asked some questions about adverse experiences in several waves of the household surveys. At first, it is the general question if the persons have already experienced an attack by a virus or similar which caused damage to the computer.

Furthermore, between 2003 and 2005, the fraudulent use of payment cards and the abuse of personal information sent on the internet has been surveyed. If SPAM email was received was also asked in 2003-2006, and with changed wording in 2006. Whether respondents have encountered any "lack of security of payments" was surveyed in 2004 only.

Similar to the Eurostat ICT household survey, there is a proposal in the review of OECD model questionnaire about experience of a virus attack which specifies further some of the circumstances involved.

Also, the revision makes two proposals about impact indicators of experienced security incidents: whether a virus (or similar) attack has actually caused a list of potential damages to the computer, such as slow-down, working halts, loss of information, etc.

Alternatively, the revision proposes to only ask about the virus having made the operations of the PC slower.

Table 4-2 Overview of existing household indicators of security incidents

Security incidents indicators	Source
Virus attack	ESTAT / CSI
Fraudulent payment card use	ESTAT
Abuse of personal information sent on the Internet	ESTAT
Spam	ESTAT
Lack of payment security in online shopping	ESTAT
Results of damage caused by an attack • The computer became significantly slower • The computer frequently stopped working or stopped working all together • Those who used the computer were sent to an unwanted Web site and/or received pop ups • Did not dial correct numbers • •Loss of files or information • Personal information was sent to others e.g. hackers	CSI
E-mail virus affecting the operation of the PC	CSI

See Annex for full description of the indicators

4.1.3 Security behaviour

The Benchmarking i2010 indicators include a measurement about security precautions. The emphasis is on updating security programs regularly for being well protected against virus attacks, for instance. Eurostat has asked in various waves about home computers being protected through virus checking programs and firewalls and if any online authentication has been used.

Eurostat also asks people to indicate how often they make safety copies of backup files from their computer to an external server. In case of a computer breakdown all data can be lost. It is advisable to make copies, particularly on important data.

In 2007, also making safety copies or back up files has been surveyed. In the skills question battery, an item "keeping viruses, spyware and adware off your computer" has been included.

Recently the Eurostat surveys also gather among their list of skill defining internet related activities also a security relevant indicator.

The Czech Statistical Institute's initial suggestions for a second review of the OECD model proposes to survey using special security programs, like a virus checking software or a firewall people can protect their computer and stored data against attacks while using the internet. Compared to the Eurostat practice, also anti-spy ware software is included.

The document also lists alternative wordings for a firewall protection. Furthermore, automatic e-mail attachments checks by such programs are proposed for inclusion.

Furthermore, regular updates of software through patches is an important security behaviour. The Czech NSI has proposed to include this in the model questionnaire. An alternative for the "frequency of backing up files" indicator is also proposed.

As an addition to Eurostat's practice, the use of automatic software updates or patches is proposed.

Table 4-3 Overview of existing household indicators of security behaviour

Security incidents indicators	Source
ICT precautions: • Virus checking program (updated/installed) • Online authentication • Firewall	ESTAT
Frequency of making safety copies of back up files	ESTAT
Internet related activities (skills) – keeping viruses off computer	ESTAT
Security programs • Virus checking or protection software • A firewall • Anti-spy ware software • Other security hardware or software	CSI /OECD
Having firewall program	CSI /OECD
Automatic virus checking of e-mails	CSI /OECD
Frequency of backing up files	CSI /OECD
Downloading software patches	CSI /OECD

See Annex for full description of the indicators

4.2 Enterprise surveys

Enterprises need to ensure the security of their data and IT infrastructure both to protect their business critical data and the data their customers have disclosed to them.

Existing indicators are presented broken down by the following categories

- Security awareness and risk assessment indicators
- Security expectations and barriers indicators
- Damage experienced, cost and impact
- Security behaviour and preventions
- Miscellaneous security indicators

4.2.1 Security awareness and risk assessment

The exposure to security threats is not only depending on the vulnerability of the IT infrastructure but of course also to the kind of data that is stored in the first place. Therefore, the UK DTI survey gathered information about whether an enterprise had highly confidential information or business critical information

Equally important is that every employee is aware of IT security. Enterprises can inform and educate its employees about their security responsibilities in different ways. However it is important that security knowledge is spread across all staff that deals with critical information. Also, security issues need to be properly prioritised in managerial staff.

Table 4-4 Overview of existing enterprise indicators of security awareness and risk assessment

Security awareness indicators	Source
Business information relevant to IT security	DTI
Assessment of organisational information security • Computer centre/mainframe • Servers • Clients/PCs • Mobile end devices (notebooks/ PDAs) • Teleworking-PCs • Storage media (Tapes, CDs, USB-memory, ...) • IT-network (wired) • IT-network, wireless (WLAN ...) • Telecoms network • Applications	kes / MS
Level of knowledge in staff • top management • middle management • IT-security staff • Users in highly sensitive areas • Users in less sensitive areas	kes / MS
Executive priority of information security	kes / MS
Open-Source-Software security assessment	kes / MS

See Annex for full description of the indicators

There are furthermore possibly some ideas to be taken out of the security guidelines, as presented in the following table.

Table 4-5 Overview of possible enterprise indicators of security awareness and risk assessment taken from security guidelines

Security awareness indicators	Source
Assessment of organisational information security • Information relating to primary business objectives • Information relating to primary business objectives • Task involving the creation, processing, storage, use and transmission of that business-critical information • Assets used to create, process, store and transmit that business-critical information • Criticality of confidentiality of assets • Criticality of integrity of assets • Criticality of availability of assets • Prioritizing assets	BIAC / ICC:

See Annex for full description of the indicators

4.2.2 Security expectations and barriers indicators

Security expectations and barriers deliver subjective indicators of IT professional as to the level of threats they feel or expect. In this sense, they can be used as a barometer of the overall security developments. Such data is most valuable when compared over time so that improvements or aggravations become observable.

Barriers indicators are also subjective assessments of what is hampering a better data protection.

Table 4-6 Overview of existing enterprise indicators of security expectations and barriers

Security expectations	
Confidence in catching breaches	DTI
Expected number of security incidents	DTI
Difficulty catching incidents in the following year	DTI
Barriers to improving IT security • Lack of awareness and support in top management • Lack of awareness in middle management • Lack of awareness of staff • Lack of basic strategic principles / general concepts • Lack of realisable specific concepts • Lack of appropriate methods and tools • Lack of opportunities for the enforcement of security relevant measures • Lack of available and qualified staff • Lack of suitable products • Applications are not prepared for information security measures • Lack of practice oriented security advisors • Lack of money • Existing concepts are not being implemented • Monitoring of compliance is insufficient • Other	kes / MS

See Annex for full description of the indicators

4.2.3 Damage experienced, cost and impact

The Eurostat ICT enterprises surveys gather whether an enterprise had encountered any of a list of three security problems in the past year. The DTI information security breaches survey gathers data on more different types of attacks, theft and fraud companies suffered from. DTI differentiates between attacks by outsiders, theft, fraud, virus infections, system failures, unwanted data disclosure, etc.

Especially, the DTI survey looks into what or who the source of such disruptions was, and what damage was caused.

Table 4-7 Overview of existing enterprise indicators of damages experienced, costs and impact

Experienced damage and impact	
Security problems in the last year	ESTAT
Kind of security problems in the last year • a) Computer virus, worm or trojan attack • b) Unauthorised access • c) Blackmail or threats to enterprise data or software	ESTAT
Attack by unauthorized outsider • Significant attempts to break into network • Actual penetration into network • Attacks on Internet or telecommunications traffic • Company impersonated on Internet (e.g. phishing attack) • Denial of service attacks	DTI
Suffering of theft and fraud • Staff used systems to commit fraud or theft • Staff stole computer equipment • Outsider stole computer equipment	DTI
Worst security incident • Virus infection and disruptive software • Systems failure or data corruption • Staff misuse of information systems • Unauthorised access by outsiders (including hacking attempts) • Physical theft of computer equipment • Theft of fraud using computers • Theft or unauthorised disclosure of confidential information • Identity theft or impersonation of the company	DTI
Source of worst malicious software incident (Virus, worm or Trojan vs. Spyware)	DTI
Number of infections	DTI
Type of virus infection	DTI
Staff misuse	DTI
Type of staff misuse • Misuse of web access • Misuse of e-mail access • Unauthorised access to systems data (e.g. using someone else's ID) • Breaches of data protection laws or regulations • Misuse of confidential information (e.g. intellectual property or customer data)	DTI

Number of misuse incidents • Misuse of web access • Misuse of e-mail access • Unauthorised access to systems or data (e.g. using someone else's ID) • Breaches of data protection laws or regulations • Misuse of confidential information (e.g. intellectual property or customer data)	DTI
Seriousness of the incidents	DTI
Reason of system failure • Human error • Network overload • Sabotage • Power supply failure • Hardware failure • Software bugs	DTI
Staff time spent to the worst security incident	DTI
Incident response costs	DTI
Financial loss	DTI
Reputation damage	DTI
Overall cost of the worst incident	DTI

See Annex for full description of the indicators

4.2.4 Security behaviour and prevention

Eurostat data on security behaviour concentrates on technical IT solutions: secure servers, firewalls, encryption, authentication, virus checking etc. The DTI surveys go further in their measurement, as they for instance include staff awareness: training measures, enterprise policies, monitoring staff behaviour and background checks of staff. They also include physical and spatial measures.

The kes survey includes a question on insurance contracts against damage from security incidents, multi-vendor strategies, open-source strategies and spatial separation.

An asset of the DTI surveys is the separation of different security domains in different questions: there are questions about website security, wireless security, email security, removable devices, physical measures, monitoring measures, staff internet access, intrusion control, among others. This way, very concrete questions can be asked to avoid ambiguous stimuli.

Table 4-8 Overview of existing enterprise indicators of security behaviour and prevention

Security behaviour and prevention	
Taking any ICT precautions **2003:** • a) Secure servers • b) Firewalls • c) Encryption for confidentiality • d) Off-site data backup • e) Authentication mechanism, Of which • e1) Electronic digital signature (as receiver) • e2) Other authentication mechanism (e.g. PIN code) • f) Virus checking or protection software • g) Subscription to a security service (e.g. virus protection or intrusion alert) **2004:** • a) Virus checking or protection software • b) Firewalls (software or hardware) • c) Secure servers • d) Off-site data backup • e) Electronic digital signature as customer's authentication mechanism • f) Other authentication mechanism (e.g. PIN code) • g) Data encryption for confidentiality **2005/2006:** • a) Virus checking or protection software • b) Firewalls (software or hardware) • c) Secure servers (support secured protocols such as shttp) • d) Off-site data backup	ESTAT
Using two or more security facilities	ESTAT
Updating of security devices	ESTAT
Adopting confidence building practices	ESTAT
Security concerns	ESTAT
Documented and defined information security policy	DTI
Making staff aware of security issues • staff handbook • specific document or leaflet • contract or letter of appointment • On joining or at induction • Training or presentations	DTI
Insurance against security threats • Electronic-/IT-property insurance • Fire insurance • Data insurance / Software insurance • Data liability insurance • Electronic-/IT-business interruption insurance • Data legal expenses insurance • Other • None having any information security reference	kes / MS
Background checks on staff	DTI
Documented procedures (UK Data Protection Act)	DTI

Monitoring of compliance with security policy • Software that detects, reacts to and records security policy violations • Monitoring activity and logging unusual events • Periodic audit of security processes • Benchmarking security processes against those in other organisations • Automated scans to check security configuration • No checks are performed	DTI
Formal security qualification	DTI
External security guidance • BS 7799 (or ISO 17799 or ISO 27001) • Guidelines issued by the government • The police • IT membership organizations (e.g. BCS, NCC, ISF or IAAC) • Your internal audit function • Your external auditors • An audit/business advisory firm other than your auditors • An IT services provider or consultancy • A security product vendor • Personal contacts within the business or security community • None	DTI
Multi-Vendor-Strategies • Anti-Virus-Software • Firewalls • Router • Server-OS • Web-Server • Application servers • Other	kes / MS
Open-Source-Software usage for security or cost reasons	kes / MS
Best method of managing risks in the future • Provision of more information security advice or information • More research of information security risk trends • Wider promotion of information security management standards • Development or promotion of technical security standards • More education for the general public about information security risks • More industry initiatives to address security risks • Nothing - there is enough being done at the moment	DTI
Physical security measures • Restrictions on access (e.g. locks) • Monitoring access (e.g. logs, CCTV) • Environmental and fire suppression control	DTI
Providing components in different premises	kes / MS
Method of precaution against disaster • Backups of critical data • Backups stored off-site • Disaster recovery plan • Disaster recovery plan tested in the last year	DTI
Frequency of backing up critical data	DTI
Software protection against viruses and malicious software • Anti-virus software • Anti-spyware software • Software that searches for probable virus activity	DTI
Frequency of updating anti-virus defences	DTI

Intrusion detection software	DTI
Web-site security solutions • Firewall • Automatic failover to backup site • Intrusion detection software • Intrusion prevention software	DTI
Wireless network security solutions • Secure placement of access points • Name of the network (service set identifier or SSID) changed from default • Encrypted signals • Connection restricted to known computers only (through MAC filtering) • No controls	DTI
Staff Internet access control • Acceptable usage policy • Internet access restricted to some staff only • Block access to inappropriate web-sites • Log and monitor web access • Scan incoming e-mail/web downloads for viruses • Filter incoming e-mail for spam • Block or quarantine suspicious e-mail attachments • Scan web downloads for spyware • Staff able to send encrypted messages to main business partners	DTI
Staff use of private systems with enterprise IT • Notebooks, PDAs etc.. (LAN/WLAN-access) • PDAs, Smartphones etc. (synchronisation with PCs) • Mobile memory (USB, firewire, digital cameras) • networks hardware (switches, WLAN-Aps, modems) • Other peripherals (e.g. printers)	kes / MS
E-mail scanning • Viruses, including Trojans • Confidential information • Inappropriate content • Unencrypted information that should be encrypted • No scans	DTI
Removable media devices precautions • Staff are told not to use such devices • Technical configuration of PCs prevents use • Confidential data is encrypted • No steps taken	DTI
Instant messaging precautions • Acceptable usage policy • Using a private and internally managed IM service • Scanning incoming messages for junk messages (spim) • Scanning outgoing messages for inappropriate content • Logging and auditing messages • Restricting which staff can use IM • No controls	DTI
IP telephony	DTI
Security expenditure	DTI
IT budget spent on IT security	DTI
Decision mechanism about spending on information security	DTI

Drivers of information security expenditure • Protecting customer information • Maintaining data integrity • Protecting the organisation's reputation • Business continuity in a disaster situation • Complying with laws and regulations • Preventing downtime and outages • Protecting other assets (e.g. cash from theft) • Improving efficiency/cost reduction • Protecting intellectual property • Enabling business opportunities	DTI
Response procedures • Logging and responding to security incidents • Maintaining evidence to legal standard • Contingency plans for dealing with possible security breaches • Procedures for dealing with claims that an outsider has taken control of network • Specialist insurance policies covering damage suffered from cybercrime or viruses	DTI
Type of security incidents planed for • Infection by malicious software • Contingency plan in place and was effective • Staff misuse of Internet or e-mail • Infringement of laws or regulations • Attack on web-site or Internet gateway • Systems failure or data corruption • Fraud or theft involving computers • Theft or unauthorised disclosure of data • Physical theft of computer equipment	DTI
Addressing the weaknesses that caused incident • Additional staff training • Changes to policies and procedures • Changes to back up and contingency plans • Changes to configuration of existing systems • Deployment of additional security technology	DTI
Regular teaching of staff • Users • Freelancers, external colleagues • Data /information processing employees • data protection commissioner • information security commissioner • Auditors • Management • Others	DTI
Teaching methods • Internal instruction through teacher centred lectures, preferably enterprise-wide • Internal instruction through teacher centred lectures, for special groups • external instruction • Learning material for self learning • Multimedia CD for self learning • Online training applications/tools	DTI

See Annex for full description of the indicators

4.2.5 Miscellaneous: Security in outsourcing

Table 4-9 Overview of existing miscellaneous enterprise indicators

Security in outsourcing	
Outsourcing of IT operations	DTI
Number of outsource arrangements	DTI
Security of offshored IT activities	DTI
Outsourcing of functions • external information security agent • entire computer centre/IT • Surveillance, monitoring, quality control • emergency provisions / business continuity • Managed Firewall/IDS/IPS • application systems • content security / virus blocking • data bank systems, tools • network management • building services • data backup solutions • data protection • documentation, archiving • destruction of data carriers (paper, IT) • personnel deployment, HR • OS maintenance, administration • other	kes / MS

See Annex for full description of the indicators

5 Proposed questionnaire modules

5.1 Household surveys

5.1.1 Security awareness and barriers

Barriers to internet home access

(from Eurostat)

What are the reasons for not having access to the Internet at home?

(Tick all that apply)

….

h) Privacy or security concerns

….

Barriers to buying online

(taken from the Benchpol report on e-commerce and trust, where also an even more comprehensive module on consumer trust in e-commerce is proposed)

Some people may fear to be taken advantage of when buying things online. Overall, how confident are you that you will not make the following adverse experience – very confident, somewhat confident, not too confident, or not at all confident?

a) That you made your payment to a fake website,

b) Non-delivery of the goods or services bought and trouble getting money back

c) Extra costs for handling or shipping claimed after the checkout process is finished.

d) Misuse of personal data you keyed in, such as selling it to spammers or address dealers.

e) Buying low quality goods because not being able to look closely at it in a physical store.

f) Redress problems

g) Forged goods, brand piracy merchandise, illegal copies or other black market goods

h) Difficulties to enforce your claims because the seller is not located in [country]

(Ask the next three questions of online buyers and of internet users who do not buy online)

In the last twelve months, has any of these fears kept you from making a planned purchase online and led you to buy in a physical store instead? (Y/N)

In the last twelve months, has any of the following features of online shopping websites kept you from making a planned purchase online and led you to buy in a physical store instead? (Y/N)

a) A website where you could not figure out the final price and fees that you would have pay before the checkout was finished.

b) A website that would not let you assess the quality of the merchandise, whether through appropriate pictures or text information.

c) A website where you could not figure out the redress conditions before the checkout was finished.

(Ask of internet users who do not buy online)

What, if any, were other reasons for not buying / ordering any goods or services for your own private use in the last 12 months? (tick all that apply)

a) Have no need

b) Prefer to shop in person, like to see product, loyalty to shops, force of habit

c) Lack of skills, you are not sure if you can handle it

d) Delivery of goods ordered at distance (internet, phone, TV or other mail-order) is a particular problem for you (e.g. takes too long or is logistically difficult) .

e) Security or privacy concerns

if yes, which of these in particular?

e1) concerns not to recognise a fake website pretending to be a renowned website

e2) concerns that an on-line seller did not send or deliver the goods or services bought or claimed not having received your payment and you had trouble getting your money back

e3) concerns that an online seller misused the personal data you key in or sold it to spammers or address dealers.

e4) concerns that an online seller sold you forged goods, brand piracy merchandise, illegal copies or other black market goods

f) You lack the trust about receiving or returning goods, or that any complaint / redress issues will be enforceable.

g) You are not sure about differences in legal provisions as to consumer rights when you want to buy from a seller not located in [country]

h) Don't have a payment card allowing to pay over the Internet

i) Speed of the Internet connection is too slow for a comfortable shopping process to be possible

j) Others

Barriers to online service usage

(new proposal)

Have security concerns kept you from using the following online services for your own private use in the last 12 months? (tick all that apply)

a) Using the Internet to communicate with public services or administrations

b) Using the Internet to carry out banking activities such as bank transfers

c) Using the Internet to communicate with a GP or other health care institution

d) Registering to online communities

e) Using the Internet from places other than home, such as from a commercial internet cafe

further applications could be added as appropriate

5.1.2 Security incidents and cost/ impact

(from CSI)

When using a computer to access the Internet at home in the last 12 (3) months, has someone in your household experienced an attack by a virus or similar (for example, a

Trojan horse or worm *[EDIT: or adware]*) which has resulted in loss of data or time, or damage to your computer (software)?

(from CSI)

Did any of the following occur as a result of damage caused by the virus or similar attack?

a) The computer became significantly slower

b) The computer frequently stopped working or stopped working all together

c) Those who used the computer were sent to an unwanted Web site and/or received pop ups

d) Did not dial correct numbers

e) Loss of files or information

f) Personal information was sent to others e.g. hackers

5.1.3 Security behaviour

(from CSI)

During the last 3 months, have you used the Internet to download any software, patches or software upgrades?

(from CSI)

When using a computer at home, how frequently did you or any member of your household back up files (such as documents, spreadsheets or digital photographs) which you created and kept on the home computer? (always or almost always, sometimes, never or hardly ever, not applicable)

(from CSI)

Are e-mails received on your home PC automatically checked for viruses?

(from CSI)

Does your home PC have a firewall program that prevents outsiders from accessing the PC via your broadband connection

(new proposal)

When using a computer at home, how frequently do you or any member of your household have a security check run on your computer to check for viruses, spyware or other malware or adware? (always or almost always, sometimes, never or hardly ever, not applicable)

5.2 Enterprise surveys

5.2.1 Security awareness and risk assessment

no proposal

5.2.2 Security expectations and barriers indicators

(from kes/Microsoft)

What kinds of problems restrict you most in improving your enterprise's information security?

a) Lack of awareness and support in top management

b) Lack of awareness in middle management

c) Lack of awareness of staff

d) Lack of basic strategic principles / general concepts

e) Lack of realisable specific concepts

f) Lack of appropriate methods and tools

g) Lack of opportunities for the enforcement of security relevant measures

h) Lack of available and qualified staff

i) Lack of suitable products

j) Applications are not prepared for information security measures

j) Lack of practice oriented security advisors

k) Lack of money

l) Existing concepts are not being implemented

m) Monitoring of compliance is insufficient

n) Other, please specify

o) None

5.2.3 Damage experienced, cost and impact

(from DTI)

Which was the worst security incident faced by your enterprise in the last year?

a) Virus infection and disruptive software

b) Systems failure or data corruption

c) Staff misuse of information systems

d) Unauthorised access by outsiders (including hacking attempts)

e) Physical theft of computer equipment

f) Theft of fraud using computers

g) Theft or unauthorised disclosure of confidential information

h) Identity theft or impersonation of the company

i) None / None of the above

How much staff time was spent responding to the worst security incident?

(to be adapted: less than a day / 1-2 person days / 3-10 person days / 11-50 person days / 50 -100 person days / more than 100 person days)

How much staff time was spent responding to security incidents, generally?

(to be adapted: less than a day / 1-2 person days / 3-10 person days / 11-50 person days / 50 -100 person days / more than 100 person days)

(adapted from DTI)

(Ask unless already mentioned in the above question as worst incident)

Did your enterprise encounter an attack to its computer system by an unauthorised outsider in the last year? (Y/N)

(Ask if yes or already mentioned in the above question as worst incident)

What kind of attack did your enterprise encounter in the last year?

a) Significant attempts to break into network

b) Actual penetration into network

c) Attacks on Internet or telecommunications traffic

d) Company impersonated on Internet (e.g. phishing attack)

e) Denial of service attacks

(adapted from DTI)

(Ask unless already mentioned in the above question as worst incident)

Did your enterprise encounter a system failure or data corruption in the last year? (Y/N)

(Ask if yes or already mentioned in the above question as worst incident)

What caused system failure or data corruption? (exact wording unavailable)

a) Human error

b) Network overload

c) Sabotage

d) Power supply failure

e) Hardware failure

f) Software bugs

5.2.4 Security behaviour

(adapted from DTI)

What percentage of your enterprise's IT budget was spent on information security, if any?

(numeric)

(adapted from DTI)

Which, if any, of the following procedures does your enterprise have in place to respond to security incidents?

a) Logging and responding to security incidents

b) Maintaining evidence to legal standard

c) Contingency plans for dealing with possible security breaches

d) Procedures for dealing with claims that an outsider has taken control of network

e) Specialist insurance policies covering damage suffered from cybercrime or viruses

(adapted from DTI)

Does your enterprise have contingency plans for any of the following security incidents ?

a) Infection by malicious software

b) Contingency plan in place and was effective

c) Staff misuse of Internet or e-mail

d) Infringement of laws or regulations

e) Attack on web-site or Internet gateway

f) Systems failure or data corruption

g) Fraud or theft involving computers

h) Theft or unauthorised disclosure of data

i) Physical theft of computer equipment

6 Annex: Existing indicator definitions

6.1 Household surveys

6.1.1 Source surveys

ESTAT: Eurostat Community Survey on ICT Usage in Households and by Individuals

The following sources were used:

- Model Questionnaires for waves 2002-2008.
- Results of the survey on the relevance of indicators for benchmarking i2010, conducted among statisticians and policy makers (2005)
- Methodological Manual for statistics on the Information Society Survey year 2007, v2.0

The EUROSTAT survey was established in close collaboration with the EU-Member states and the OECD. The European Commission established annual information Society surveys to benchmark the ICT-driven development in enterprises and by individuals form 2002 on.

CSI /OECD: Czech Statistical Institute - Working Party on Indicators for the Information Society

WPIIS 2007 room document: ICT access and use by households and individuals: initial suggestions for a second review of the OECD model questionnaire (2007)

This report shows available data and an OECD model questionnaire for the member states to adopt in their own survey. There are also businesses and households asked for their ICT usage and trust in the online environment.

6.1.2 Indicator descriptions

Security awareness and opinions

Name of Indicator	**Security concerns as barrier to home internet access**
Definition	Percentage of individuals stating that security or privacy concerns are a reason for them to not have internet access at home
Notes	
Question wording	2002-2004: What are the main reasons for you not having access to the Internet at home? 2005, 2006, 2008: What are the reasons for not having access to the Internet at home? (Tick all that apply) h) Privacy or security concerns
Source	Eurostat waves 2002-206, 2008
Results available	Eurostat

Name of Indicator	**Security concerns as barrier to buying online**
Definition	Percentage of individuals stating that security concerns are a reason for them to not buy online
Notes	
Question wording	What were the (*2002-2005:* main) reasons for not buying / ordering any goods or services for your own private use (2005, 2006: in the last 12 months)? … h) Security concerns, worried about giving credit card details over the Internet *2006: e) Security or privacy concerns*
Source	Eurostat waves 2002, 2003
Results available	Eurostat

Name of Indicator	**Privacy concerns as barrier to buying online**
Definition	Percentage of individuals stating that privacy concerns are a reason for them to not buy online
Notes	*2006 merged with the above question*
Question wording	What were the (*2002-2005:* main) reasons for not buying / ordering any goods or services for your own private use (2005, 2006: in the last 12 months)? … i) Privacy concerns / worried about giving personal details over the Internet *2006 merged with the above question*
Source	Eurostat waves 2002, 2003
Results available	Eurostat

Name of Indicator	**Trust concerns as barrier to buying online**
Definition	Percentage of individuals stating that trust concerns are a reason for them to not buy online
Notes	
Question wording	What were the (*2002-2005:* main) reasons for not buying / ordering any goods or services for your own private use (2005, 2006: in the last 12 months)? … j) Trust concerns / concerned about receiving or returning goods *2005, 2006: j) Trust concerns about receiving or returning goods, complaint / redress concerns*
Source	Eurostat waves 2002, 2003
Results available	Eurostat

Name of Indicator	**Complaint / redress concerns as barrier to buying online**
Definition	Percentage of individuals stating that complaint / redress concerns are a reason for them to not buy online
Notes	*2005, 2006: merged with above indicato*r
Question wording	What were the (*2002-2005:* main) reasons for not buying / ordering any goods or services for your own private use (2005, 2006: in the last 12 months)? … k) Complaint / redress concerns, worried about difficulty for redress *2005, 2006: merged with above indicato*r
Source	Eurostat waves 2002, 2003
Results available	Eurostat

Name of Indicator	**Security concerns as barrier to e-government**
Definition	Percentage of individuals stating that security concerns are a reason for them to not use e-government
Notes	
Question wording	D2 What are the reasons for not using the Internet for dealing with public services or administrations? (tick all that apply) d) Concerned about protection and security of my data
Source	Eurostat waves 2006
Results available	Eurostat

Name of Indicator	**Security concerns as barrier to more intense internet use**
Definition	Percentage of individuals stating that security concerns are a reason for them to not use the internet more
Notes	(Filter: if internet user and wanting to use internet more)
Question wording	C9 What are your barriers to more intensive use of the internet (tick all that apply) h) security of privacy concerns
Source	Eurostat waves 2007
Results available	Eurostat

Security incidents

Name of Indicator	**Virus attack**
Definition	Persons having a computer virus through using the internet.
Notes	Benchmarking i2010 indicator (partly)
Question wording	*2007:* Through using the Internet, have you had a computer virus resulting in loss of information or time in the last 12 months? *2003 -2005:* In the last 12 months, have you encountered any of the following security problems through using the Internet? a) Computer virus resulting in loss of information or time
Source	Eurostat ICT household surveys, waves 2007, 2003-2005
Results available	Eurostat

Name of Indicator	**Virus attack**
Definition	Persons having experienced an attack by a virus or similar which has resulted in loss of data or time, or damage to your computer.
Notes	
Question wording	When using a computer to access the Internet at home in the last 12 (3) months, has someone in your household experienced an attack by a virus or similar (for example, a Trojan horse or worm) which has resulted in loss of data or time, or damage to your computer (software)?
Source	Czech Statistical Institute - WPIIS 2007 room document.: ICT access and use by households and individuals: initial suggestions for a second review of the OECD model questionnaire (2007) – Q8
Results available	--

Name of Indicator	**Fraudulent payment card use**
Definition	Persons having encountered fraudulent payment card use through using the internet.
Notes	Benchmarking i2010 indicator (partly)
Question wording	*2003 -2005:* In the last 12 months, have you encountered any of the following security problems through using the Internet? b) Fraudulent payment (credit or debit) card use
Source	Eurostat ICT household surveys, waves 2003-2005
Results available	Eurostat

Name of Indicator	**Abuse of personal information sent on the Internet**
Definition	Persons having encountered abuse of personal information sent on the Internet through using the internet.
Notes	Benchmarking i2010 indicator (partly)
Question wording	*2003 -2005:* In the last 12 months, have you encountered any of the following security problems through using the Internet? c) Abuse of personal information sent on the Internet
Source	Eurostat ICT household surveys, waves 2003-2005
Results available	Eurostat

Name of Indicator	**Spam**
Definition	Persons having received unsolicited e-mails.
Notes	Benchmarking i2010 indicator (partly)
Question wording	*2006: In the last 3 months, did you receive unsolicited e-mails that you would regard as junk mail or spam and that you would prefer not to receive? (Y/N)* *2003 -2005:* In the last 12 months, have you encountered any of the following security problems through using the Internet? d) ‘Spam’ – unsolicited emails sent to you
Source	Eurostat ICT household surveys, wave 2006, 2003-2005
Results available	Eurostat

Name of Indicator	**Lack of payment security in online shopping**
Definition	Persons having encountered lack of security of payments when making orders over the internet
Notes	
Question wording	What problems (*2004:* , if any,) have you encountered when making orders over the Internet? … g) Lack of security of payments
Source	Eurostat ICT household surveys, waves 2004-2006
Results available	Eurostat

Name of Indicator	**Results of damage caused by an attack**
Definition	Persons having experienced different effects on their computer after a virus or similar attack.
Notes	*Supplementary Question* Multiple answers possible
Question wording	Did any of the following occur as a result of damage caused by the virus or similar attack? • The computer became significantly slower • The computer frequently stopped working or stopped working all together • Those who used the computer were sent to an unwanted Web site and/or received pop ups • Did not dial correct numbers • Loss of files or information • Personal information was sent to others e.g. hackers
Source	Czech Statistical Institute - WPIIS 2007 room document.: ICT access and use by households and individuals: initial suggestions for a second review of the OECD model questionnaire (2007)
Results available	"NZE 2006"

Name of Indicator	**E-mail virus affecting the operation of the PC**
Definition	Persons having experienced that e-mail viruses affected the operation of their home PC during the past six month.
Notes	
Question wording	Have e-mail viruses affected the operation of your home PC during the past six months? (never, once or twice, more often)
Source	Czech Statistical Institute - WPIIS 2007 room document.: ICT access and use by households and individuals: initial suggestions for a second review of the OECD model questionnaire (2007)
Results available	"NZE 2006"

Security behaviour

Name of Indicator	**ICT precautions: Virus checking program**
Definition	Persons who installed or updated a virus checking program within the last 3 month.
Notes	Benchmarking i2010 indicator Deemed inappropriate as a result of the survey on the relevance of indicators for benchmarking i2010, conducted among statisticians and policy makers (2005)
Question wording	In the last 3 months, have you taken any of the following security precautions? a) Installed a virus checking program (2003, 2004) b) Updated a virus checking program(2003) b) Updated a virus checking program (including automatic updating) (2004) 2005: Is the device you use to access the Internet at home protected by a) a virus checking program? Has it been installed or updated in the last 3 months (incl. automatic updating)?
Source	Eurostat ICT household surveys, waves 2003-2005
Results available	Eurostat

Name of Indicator	**ICT precautions: Online authentication**
Definition	Persons who used online authentication within the last 3 month.
Notes	Benchmarking i2010 indicator Deemed inappropriate as a result of the survey on the relevance of indicators for benchmarking i2010, conducted among statisticians and policy makers (2005)
Question wording	In the last 3 months, have you taken any of the following security precautions? c) Used online authentication (such as a password, PIN, or a digital signature) on the Internet (2003, 2004) 2005: In the last 3 months, have you used online authentication on the Internet for private use. such as a password, PIN or digital signature?
Source	Eurostat ICT household surveys, waves 2003-2005
Results available	Eurostat

Name of Indicator	**ICT precautions: Firewall**
Definition	Persons who installed or upgraded a software or hardware firewall within the last 3 month.
Notes	Benchmarking i2010 indicator Deemed inappropriate as a result of the survey on the relevance of indicators for benchmarking i2010, conducted among statisticians and policy makers (2005)
Question wording	In the last 3 months, have you taken any of the following security precautions? d) Installed or upgraded a hardware or software firewall (2004) 2005: Is the device you use to access the Internet at home protected by a) a hardware or software firewall? Has it been installed or updated in the last 3 months (incl. automatic updating)?
Source	Eurostat ICT household surveys, waves 2003-2005
Results available	Eurostat

Name of Indicator	**Frequency of making safety copies of back up files**
Definition	Persons who state the frequency of making safety copies of back up files from their computer.
Notes	
Question wording	How often do you make safety copies or back up files (documents, pictures, etc.) from your computer on e.g. a diskette, a CD or to diskspace on Internet servers?
Source	Eurostat ICT household surveys, wave 2007
Results available	Eurostat

Name of Indicator	**Internet related activities (skills) – keeping viruses off computer**
Definition	Persons who state which internet related activities they've already carried out.
Notes	Multiple answers possible
Question wording	Which of the following Internet related activities have you already carried out? • … • Keeping viruses, spyware and adware off your computer
Source	Eurostat ICT household surveys, wave 2007
Results available	Eurostat

Name of Indicator	**Security programs**
Definition	Persons having their computer used to access the internet protected
Notes	Multiple answers possible
Question wording	Is the computer(s) used to access the Internet at home protected by • Virus checking or protection software? • A firewall? • Anti-spy ware software? • Other security hardware or software (please specify)
Source	Czech Statistical Institute - WPIIS 2007 room document. ICT access and use by households and individuals: initial suggestions for a second review of the OECD model questionnaire (2007) – Q7
Results available	No

Name of Indicator	**Having firewall program**
Definition	Persons having a firewall program on their home PC which prevents outsiders from accessing the PC via their broadband connection.
Notes	*Supplementary indicator*
Question wording	Does your home PC have a firewall program that prevents outsiders from accessing the PC via your broadband connection?
Source	Czech Statistical Institute - WPIIS 2007 room document. ICT access and use by households and individuals: initial suggestions for a second review of the OECD model questionnaire (2007)
Results available	"FIN 2004"

Name of Indicator	**Automatic virus checking of e-mails**
Definition	Persons having received e-mails automatically checked for viruses.
Notes	*Supplementary indicator*
Question wording	Are e-mails received on your home PC automatically checked for viruses?
Source	Czech Statistical Institute - WPIIS 2007 room document ICT access and use by households and individuals: initial suggestions for a second review of the OECD model questionnaire (2007)
Results available	FIN 2004

Name of Indicator	**Frequency of backing up files**
Definition	Frequency of backing up created files that are kept on home computer.
Notes	
Question wording	When using a computer at home, how frequently did you or any member of your household back up files (such as documents, spreadsheets or digital photographs) which you created and kept on the home computer? (always or almost always, sometimes, never or hardly ever, not applicable)
Source	Czech Statistical Institute - WPIIS 2007 room document ICT access and use by households and individuals: initial suggestions for a second review of the OECD model questionnaire (2007) – Q9
Results available	no

Name of Indicator	**Downloading software patches**
Definition	Persons who used the internet to download any software, patches or software upgrades during the last 3 month.
Notes	
Question wording	During the last 3 months, have you used the Internet to download any software, patches or software upgrades?
Source	Czech Statistical Institute - WPIIS 2007 room document ICT access and use by households and individuals: initial suggestions for a second review of the OECD model questionnaire (2007)
Results available	no

6.2 Enterprise surveys

6.2.1 Source surveys

DTI: dti information security breaches survey 2006, technical report (enterprises)

Between October 2005 and January 2006 the Information Security Breaches Survey (ISBS 2006) took place. Businesses in the United Kingdom were interviewed in computer-assisted telephone interviews which lasted about 30 minutes. The ISBS has been the eight such survey managed by PricewaterhouseCoopers.

Since 1991 the Department of Trade and Industry has sponsored research into information security breaches. Their intention is to inform UK businesses about the potential risks of IT usage.

kes/MS: <kes>/Microsoft-Sicherheitsstudie 2006

The Microsoft Germany company has send out questionnaires to private and small or entrepreneurial companies in Germany. There were 163 enterprises taking part in the survey in 2006. The magazine for information-security <kes> asks for experiences enterprises made while using their IT equipment and even wants to know how secure their network and data are. There is also a checklist implied by the questionnaire with the intention of businesses' self-estimation towards their security situation while filling out. The answered questionnaire should have been send back to <kes> till the 1st of May 2006.

There have also been surveys from kes/Microsoft before. This one was based on the KES/Microsoft-security study in 2004 and the KES/KMPG-security study in 2002. In the study comparisons to the older results have been made and investigating which expectations became valid.

This study was supported by companies like SAP, itWatch GmbH or Sonicwall. Microsoft cooperates with 14 companies since 2004 to do these studies.

ESTAT: Eurostat Community Survey on ICT Usage and e-Commerce in Enterprises

The following sources were used:

- Model Questionnaires for waves 2002-2008.
- Results of the survey on the relevance of indicators for benchmarking i2010, conducted among statisticians and policy makers (2005)
- Methodological Manual for statistics on the Information Society Survey year 2007, v2.0

The EUROSTAT survey was established in close collaboration with the EU-Member states and the OECD. The European Commission established annual information Society surveys to benchmark the ICT-driven development in enterprises and by individuals form 2002 on.

BIAC / ICC: *Securing your business - A companion for small or entrepreneurial companies to the 2002 OECD Guidelines for the security of networks and information systems: Towards a culture of security*

This guide was published in July 2004 by the Business and Industry Advisory Committee to the OECD (BIAC) and the International Chamber of Commerce. It is addressed to small and entrepreneurial companies with limited information technology resources.

6.2.2 Indicator descriptions

Security awareness and risk assessment

Name of Indicator	**Business information relevant to IT security**
Definition	UK businesses that have certain information that is relevant to IT security
Notes	
Question wording	Does the business have information that: *(exact wording unavailable)* • Is highly confidential? • Would cause significant business disruption if corrupted? • Would cause significant business disruption if not available?
Source	DTI information **security** breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Assessment of organisational information security**
Definition	Assessment of information security by firms.
Notes	
Question wording	*(translation from German)* How would you assess the information security in your house? As regards … (Wie schätzen Sie die Informationssicherheit (ISi) in Ihrem Haus ein? bezogen auf ...) • Computer centre/mainframe (Rechenzentrum/Mainframe) • Servers (Server) • Clients/PCs (Clients/PCs) • Mobile end devices (notebooks/ PDAs) (mobile Endgeräte (Notebooks, PDAs, ...)) • Teleworking-PCs (Teleworking-PCs) • Storage media (Tapes, CDs, USB-memory, ...)(Speichermedien (Tapes, CDs, USB-Speicher, ...)) • IT-network (wired) (IT-Netzwerk (kabelgebunden)) • IT-network, wireless (WLAN ...) (IT-Netzwerk, drahtlos (WLAN ...)) • Telecoms network (TK-Netzwerk) • Applications (Applikationen/Geschäftsanwendungen)
Source	<kes>/Microsoft-Sicherheitsstudie 2006
Pilot results available	

Name of Indicator	**Level of knowledge with regard to IT security in staff**
Definition	Assessment of knowledge regarding IT security in different staff groups.
Notes	
Question wording	How would you assess the level of knowledge with regard to Information Security in your house? *(translation from German)* (Wie beurteilen Sie den Kenntnisstand zur ISi in Ihrem Hause?) Very good / good / satisfactory / sufficient / not sufficient / not answerable (sehr gut/ gut/ befriedigend/ ausreichend/ nicht ausreichend/ nicht beantwortbar bezogen auf...) • top management (Top-Management) • middle management (Mittelmanagemen)t • IT-security staff (IT-Sicherheitsfachleute) • Users in highly sensitive areas (Anwender in hochsensitiven Bereichen) • Users in less sensitive areas (Anwender in weniger sensitiven Bereichen)
Source	<kes>/Microsoft-Sicherheitsstudie 2006
Pilot results available	

Name of Indicator	**Executive priority of information security**
Definition	Level of priority of information security in top management or director groups.
Notes	
Question wording	How high a priority is information security to top management or director groups? *(exact wording unavailable)*
Source	DTI information **security** breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Open-Source-Software security assessment**
Definition	Businesses that state the expected security of Open-Source-Software and even use them.
Notes	
Question wording	*(translation from German)* (a) How would you assess the security of open-source-software compared to products with non-disclosed source code? (Wie schätzen Sie die Sicherheit von Open-Source-Software im Vergleich zu Produkten mit nicht-offengelegtem Quelltext ein?) • significantly more secure (erheblich sicherer) • somewhat more secure (etwas sicherer) • equally secure (gleich sicher) • less secure (weniger sicher) • significantly less secure (erheblich unsicherer) • not answerable (nicht beantwortbar)
Source	<kes>/**Microsoft**-Sicherheitsstudie 2006
Pilot results available	

Security awareness indicator ideas taken from enterprise guidelines

Name of Indicator	**Information relating to primary business objectives**
Definition	
Notes	
Question wording	How does the information you use in your business relate to your primary business objectives?
Source	BIAC / ICC 2004: Securing your business - An companion for small or entrepreneurial companies to the 2002 OECD Guidelines for the security of networks and information systems: Towards a culture of security
Pilot results available	

Name of Indicator	**Identifying critical information**
Definition	
Notes	
Question wording	Have you identified the information that is critical for you to do business?
Source	BIAC / ICC 2004: Securing your business - An companion for small or entrepreneurial companies to the 2002 OECD Guidelines for the security of networks and information systems: Towards a culture of security
Pilot results available	

Name of Indicator	**Task involving the creation, processing, storage, use and transmission of that business-critical information**
Definition	Type of tasks performing that involve the creation, processing, storage, use and transmission, as share of businesses having identified critical information.
Notes	
Question wording	What tasks do you perform that involve the creation, processing, storage, use and transmission of that business-critical information?
Source	BIAC / ICC 2004: Securing your business - An companion for small or entrepreneurial companies to the 2002 OECD Guidelines for the security of networks and information systems: Towards a culture of security
Pilot results available	

Name of Indicator	**Assets used to create, process, store and transmit that business-critical information**
Definition	Businesses that state the type of assets used to create, process, store and transmit critical information.
Notes	
Question wording	What assets do you use to create, process, store and transmit that business-critical information (for example computers, card-indexes, mobile phones)?
Source	BIAC / ICC 2004: Securing your business - An companion for small or entrepreneurial companies to the 2002 OECD Guidelines for the security of networks and information systems: Towards a culture of security
Pilot results available	

Name of Indicator	**Criticality of confidentiality of assets**
Definition	
Notes	
Question wording	Do you know what would happen to your business if the confidentiality of those assets was compromised (if, say, a competitor gained access to them)?
Source	BIAC / ICC 2004: Securing your business - An companion for small or entrepreneurial companies to the 2002 OECD Guidelines for the security of networks and information systems: Towards a culture of security
Pilot results available	

Name of Indicator	**Criticality of integrity of assets**
Definition	
Notes	
Question wording	Do you know what would happen to your business if the integrity of those assets was compromised, and you were unable to trust the information in them?
Source	BIAC / ICC 2004: Securing your business - An companion for small or entrepreneurial companies to the 2002 OECD Guidelines for the security of networks and information systems: Towards a culture of security
Pilot results available	

Name of Indicator	**Criticality of availability of assets**
Definition	
Notes	
Question wording	Do you know what would happen to your business if those assets were unavailable to you for a period of an hour, a day, a week or a month?
Source	BIAC / ICC 2004: Securing your business - An companion for small or entrepreneurial companies to the 2002 OECD Guidelines for the security of networks and information systems: Towards a culture of security
Pilot results available	

Name of Indicator	**Prioritizing assets**
Definition	
Notes	
Question wording	Using what you now know about the confidentiality, integrity and availability of your company's information assets, can you prioritise them?
Source	BIAC / ICC 2004: Securing your business - An companion for small or entrepreneurial companies to the 2002 OECD Guidelines for the security of networks and information systems: Towards a culture of security
Pilot results available	

Security expectations and barriers indicators

Name of Indicator	**Confidence in catching breaches**
Definition	UK businesses level of confidence in catching all significant breaches that occurred in the last year.
Notes	
Question wording	How confident are UK businesses that they have caught all significant breaches that occurred in the last year? *(exact wording unavailable)*
Source	DTI information **security** breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Expected number of security incidents**
Definition	UK businesses that state the expected number of security incidents in the next year.
Notes	
Question wording	How many security incidents do UK businesses expect next year compared with last? *(exact wording unavailable)*
Source	DTI information **security** breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Difficulty catching incidents in the following year**
Definition	Assessment of the difficulty of catching security incidents in the following year.
Notes	
Question wording	Will it be more or less difficult to catch security incidents next year? *(exact wording unavailable)*
Source	DTI information **security** breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Barriers to improving IT security**
Definition	Barriers to improving IT security.
Notes	Multiple answers possible
Question wording	What kinds of problems restrict you most in improving information security? *(translation from German)* (Welche Probleme behindern Sie am meisten bei der Verbesserung der ISi?) • Lack of awareness and support in top management (Es fehlt an Bewusstsein und Unterstützung im Top-Management) • Lack of awareness in middle management (Es fehlt an Bewusstsein beim mittleren Management) • Lack of awareness of staff (Es fehlt an Bewusstsein bei den Mitarbeitern) • Lack of basic strategic principles / general concepts (Es fehlen die strategischen Grundlagen / Gesamt-Konzepte) • Lack of realisable specific concepts (Es fehlen realisierbare (Teil-)Konzepte) • Lack of appropriate methods and tools (Es fehlen geeignete Methoden und Werkzeug) • Lack of opportunities for the enforcement of security relevant measures (Es fehlt an Möglichkeiten zur *Durchsetzung* sicherheitsrelevanter Maßnahmen) • Lack of available and qualified staff (Es fehlen verfügbare und kompetente Mitarbeiter) • Lack of suitable products (Es fehlen geeignete Produkte) • Applications are not prepared for information security measures (Anwendungen sind nicht für ISi-Maßnahmen vorbereitet) • Lack of practice oriented security advisors (Es fehlt an praxisorientierten Sicherheitsberatern) • Lack of money (Es fehlt an Geld) • Existing concepts are not being implemented (Die vorhandenen Konzepte werden nicht umgesetzt) • Monitoring of compliance is insufficient (Die Kontrolle auf Einhaltung ist unzureichend) • Other, please specify (Sonstiges (bitte nennen)) • None (keine)
Source	<kes>/Microsoft-Sicherheitsstudie 2006
Pilot results available	

Damage experienced, cost and impact

Name of Indicator	**Security problems in the last year**
Definition	Enterprises that have encountered security problems in the last year.
Notes	
Question wording	Did your enterprise encounter any ICT related security problems in the last 12 months? (2005 -> follow up if yes, see below)
	Did your enterprise encounter ICT related security problems during 2005 (e.g. computer virus, worms or trojan attack, unauthorised external access to the computer system), that resulted in a loss of information or working time? (2006)
Source	Eurostat ICT enterprise surveys, waves 2005, 2006
Pilot results available	

Name of Indicator	**Kind of security problems in the last year**
Definition	Specification of encountered security problems in the last year.
Notes	
Question wording	Did your enterprise encounter the following ICT related security problems in the last 12 months? • a) Computer virus, worm or trojan attack resulting in loss of information or working time • b) Unauthorised access to enterprise computer systems or data • c) Blackmail or threats to the enterprise data or software
Source	Eurostat ICT enterprise surveys, waves 2005
Pilot results available	

Name of Indicator	**Attack by unauthorized outsider**
Definition	UK businesses that were attacked by an unauthorized outsider in the last year.
Notes	Multiple answers possible
Question wording	(How many UK businesses were) attacked by an unauthorised outsider in the last year? *(exact wording unavailable)* • Significant attempts to break into network • Actual penetration into network • Attacks on Internet or telecommunications traffic • Company impersonated on Internet (e.g. phishing attack) • Denial of service attacks • Any of the above
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Suffering of theft and fraud**
Definition	UK businesses that state the type of theft and fraud they suffered.
Notes	Multiple answers possible
Question wording	What type of theft and fraud did UK businesses suffer? • Staff used systems to commit fraud or theft • Staff stole computer equipment • Outsider stole computer equipment • Any of the above
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Worst security incident**
Definition	UK businesses that state the worst security incident.
Notes	
Question wording	What was the worst security incident faced (by UK businesses)? *(exact wording unavailable)* • Virus infection and disruptive software • Systems failure or data corruption • Staff misuse of information systems • Unauthorised acces by outsiders (including hacking attempts) • Physical theft of computer equipment • Theft of fraud using computers • Theft or unauthorised disclosure of confidential information • Identity theft or impersonation of the company
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Source of worst malicious software incident**
Definition	UK businesses that state the source of the worst malicious software incident.
Notes	
Question wording	What was the source of the worst malicious software incident? *(exact wording unavailable)* • Virus, worm or Trojan • Spyware
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Number of infections**
Definition	Number of infections, as share of all businesses being affected, stated by UK businesses.
Notes	
Question wording	How many infections did (the affected businesses) suffer in the last year? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Type of virus infection**
Definition	UK businesses that state the reason of the worst virus infection.
Notes	
Question wording	What caused the worst virus infections? *(exact wording unavailable)* • Netsky • MyDoom • Zafi/Erkez • Bagle/Beagle • Sober • Others
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Staff misuse**
Definition	UK businesses having suffered from staff misuse of information systems.
Notes	
Question wording	(How many UK businesses have) suffered from staff misuse of information systems? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Type of staff misuse**
Definition	UK businesses that state the type of staff misuse they've suffered from.
Notes	
Question wording	What type of staff misuse (did UK businesses) suffer? *(exact wording unavailable)* • Misuse of web access • Misuse of e-mail access • Unauthorised access to systems data (e.g. using someone else's ID) • Breaches of data protection laws or regulations • Misuse of confidential information (e.g. intellectual property or customer data) • Any of the above
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Number of misuse incidents**
Definition	UK businesses that state the number of misuse incidents, as share of being affected.
Notes	
Question wording	How many misuse incidents (did affected UK businesses) suffer? *(exact wording unavailable)* • Misuse of web access • Misuse of e-mail access • Unauthorised access to systems or data (e.g. using someone elses's ID) • Breaches of data protection laws or regulations • Misuse of confidential information (e.g. intellectual property or customer data) • One only • A few • Roughly one a month • Roughly one a week • Roughly one a day • Several a day • Hundreds a day
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Seriousness of the incidents**
Definition	Seriousness of the incidents as perceived by UK businesses that state these.
Notes	
Question wording	How serious were different types of incident? *(exact wording unavailable)* • Extremely serious • Very serious • Serious • Not serious • Not all serious
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Reason of system failure**
Definition	Reason of system failure or data corruption.
Notes	
Question wording	What caused system failure or data corruption? *(exact wording unavailable)* • Human error • Network overload • Sabotage • Power supply failure • Hardware failure • Software bugs
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Staff time spent to the worst security incident.**
Definition	Staff time spent to the worst security incident.
Notes	
Question wording	How much staff time was spent responding to the worst security incident? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Incident response costs**
Definition	Cash expenditure required from the worst incident.
Notes	
Question wording	How much cash expenditure was required to recover from the worst incident? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Financial loss**
Definition	Expenditure of the direct financial loss associated with the worst case.
Notes	
Question wording	What was the direct financial loss associated with the worst incident? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Reputation damage**
Definition	Extent to which the worst incident damaged the reputation of the business.
Notes	
Question wording	To what extent did the worst incident damage the reputation of the business? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Overall cost of the worst incident**
Definition	Overall cost of a company’s worst incident in the last year.
Notes	
Question wording	What was the overall cost of a company’s worst incident in the last year? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Security behaviour and prevention

Name of Indicator	**Taking any ICT precautions**
Definition	Enterprises that took ICT precautions. Defined as firewalls, encryption for confidentiality, off-site data backup, authentication mechanism, virus checking or protection software, subscription to a security service
Notes	eEurope Benchmarking indicator, however results of the survey on the relevance of indicators for benchmarking i2010, conducted among statisticians and policy makers (2005) suggests to drop this indicator
Question wording	Which of the following security facilities does your enterprise use? (Multiple choice) **2003:** • a) Secure servers • b) Firewalls • c) Encryption for confidentiality • d) Off-site data backup • e) Authentication mechanism Of which • e1) Electronic digital signature (as receiver) • e2) Other authentication mechanism (e.g. PIN code) • f) Virus checking or protection software • g) Subscription to a security service (e.g. virus protection or intrusion alert) • 2004: question ditto • a) Virus checking or protection software • b) Firewalls (software or hardware) • c) Secure servers • d) Off-site data backup • e) Electronic digital signature as customer's authentication mechanism • f) Other authentication mechanism (e.g. PIN code) • g) Data encryption for confidentiality **2005/2006: Did your enterprise use the following internal security facilities, during January 2005(2006)** • a) Virus checking or protection software • b) Firewalls (software or hardware) • c) Secure servers (support secured protocols such as shttp) • d) Off-site data backup
Source	Eurostat ICT enterprise surveys, wave 2003 -2006
Pilot results available	Eurostat

Name of Indicator	**Using two or more security facilities**
Definition	Enterprises that use at least two security facilities.
Notes	eEurope Benchmarking indicator, supplementary to previous one.
Question wording	*Compound indicator using data from above set of questions*
Source	Eurostat ICT enterprise surveys, wave 2003 -2006
Pilot results available	

Name of Indicator	**Updating of security devices**
Definition	Enterprises having installed security devices on their PCs and updated them within the last three month.
Notes	eEurope Benchmarking indicator, however results of the survey on the relevance of indicators for benchmarking i2010, conducted among statisticians and policy makers (2005) suggests to drop this indicator
Question wording	2003, 2004 Has the enterprise updated any of its security facilities (e.g. virus protection software) in the last 3 months? (2004 add:(This includes automatic updates)) 2005 Did your enterprise update any of its security facilities (e.g. virus protection software) in the last 3 months? (This includes automatic updates).
Source	Eurostat ICT enterprise surveys, wave 2003 -2005
Pilot results available	Eurostat

Name of Indicator	**Adopting confidence building practices**
Definition	Enterprises adopting confidence building practices.
Notes	Suggested additional eEurope Benchmarking indicator, however results of the survey on the relevance of indicators for benchmarking i2010, conducted among statisticians and policy makers (2005) suggests to drop this indicator
Question wording	Did your enterprise use the following practices and informs about this on its website, during January 2005? (Yes No) a) Trust marks b) Alternative dispute resolution mechanisms (resolution via an impartial outsider) c) Customer service/ complaints mechanisms
Source	Eurostat ICT enterprise surveys, wave 2005, optional question.
Pilot results available	Eurostat

Name of Indicator	**Security concerns**
Definition	Enterprises having security concerns.
Notes	Proposal for a new benchmarking indicator. However results of the survey on the relevance of indicators for benchmarking i2010, conducted among statisticians and policy makers (2005) suggests not to adopt this proposed indicator
Question wording	*Wording unclear*
Source	Results of the survey on the relevance of indicators for benchmarking i2010, conducted among statisticians and policy makers (2005)
Pilot results available	

Name of Indicator	**Documented and defined information security policy**
Definition	UK businesses that have a formally documented and defined information security policy, as share of all businesses using computers.
Notes	
Question wording	(How many UK businesses have) a formally documented and defined information security policy? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Making staff aware of security issues**
Definition	UK businesses making their staff aware of their obligations regarding security issues
Notes	Multiple answers possible
Question wording	(How do UK businesses) make their staff aware of their obligations regarding security issues? *(exact wording unavailable)* • Via the staff handbook • Via a specific document or leaflet • Through their contract or letter of appointment • On joining or at induction • Through training or presentations • None of the above
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Insurance against security threats**
Definition	Businesses having an insurance contract in different sectors and state whether they have already used it.
Notes	
Question wording	Which insurances in the area of information security has your house effected / made claims on? *(translation from German)* (effected Y/N; if yes: made claims on Y/N) • Electronic-/IT-property insurance (Elektronik/ IT-Sachversicherung) • Fire insurance (Feuerversicherung) • Data insurance / Software insurance (Datenversicherung/Softwareversicherung) • Data liability insurance (Datenhaftpflicht-Versicherung) • Electronic-/IT-business interruption insurance (Elektronik-/IT-Betriebsunterbrechungsversicherung) • Data legal expenses insurance (Datenrechtsschutz-Versicherung) • Other (Sonstige) • None having an information security reference (keine mit ISi-Bezug)
Source	KES / Microsoft-Sicherheitsstudie 2006
Pilot results available	

Name of Indicator	**Background checks on staff**
Definition	UK businesses that do at least sometimes carry out background checks on staff and potential staff.
Notes	
Question wording	(How often do UK businesses) carry out background checks on staff and potential staff? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Documented procedures (UK Data Protection Act)**
Definition	UK businesses having documented procedures to ensure compliance with the Data Protection Act.
Notes	
Question wording	(Do UK businesses) have documented procedures to ensure compliance with the Data Protection Act? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Monitoring of compliance with security policy**
Definition	UK businesses that state certain possibilities for monitoring compliance with their security policy.
Notes	Multiple answers possible
Question wording	(How do UK businesses) monitor compliance with their security policy? *(exact wording unavailable)* • Software that detects, reacts to and records security policy violations • Monitoring activity and logging unusual events • Periodic audit of security processes • Benchmarking security processes against those in other organisations • Automated scans to check security configuration • No checks are performed
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Formal security qualification**
Definition	(UK businesses that have) any formal security qualification for their team responsible for information security.
Notes	
Question wording	Does the team responsible for information security have any formal security qualifications? *(exact wording unavailable)*
Source	DTI information **security** breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**External security guidance**
Definition	UK businesses that state what external security guidance and expertise have UK businesses drawn on in the last year.
Notes	
Question wording	What external security guidance and expertise have UK businesses drawn on in the last year? • BS 7799 (or ISO 17799 or ISO 27001) • Guidelines issued by the government • The police • IT membership organizations (e.g. BCS, NCC, ISF or IAAC) • Your internal audit function • Your external auditors • An audit/business advisory firm other than your auditors • An IT services provider or consultancy • A security product vendor • Personal contacts within the business or security community • None
Source	DTI information **security** breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Multi-Vendor-Strategies**
Definition	Businesses using security products of different provider.
Notes	Multiple answers possible
Question wording	*(translation from German)* Do you, for security reasons, use in different systems or network segments products of multiple or different vendors? (Nutzen Sie aus Sicherheitsgründen auf verschiedenen Systemen oder Netzwerksegmenten Produkte mehrerer oder verschiedener Anbieter?) Answer categories per item: Deployment of products of one, two three or more providers , not answerable (Einsatz von Produkten von nur einem; zweier; von drei o. mehr; n. b. Anbieter(n)) • Anti-Virus-Software • Firewalls • Router • Server-OS (Server-Betriebssysteme) • Web-Server • Application servers (Applikations-Server) • Other (Sonstiges)
Source	<kes>/Microsoft-Sicherheitsstudie 2006
Pilot results available	

Name of Indicator	**Open-Source-Software usage for security or cost reasons**
Definition	Businesses that state the expected security of Open-Source-Software and even use them.
Notes	
Question wording	*(translation from German)* (b) Does your enterprise deploy open-source software? (Setzt Ihr Unternehmen Open-Source-Software ein?) • yes, for cost reasons (ja, aus Kostengründen) • yes, for security reasons (ja, aus Sicherheitsgründen) • yes, because *specify* (ja, wegen:) • no (nein)
Source	<kes>/**Microsoft**-Sicherheitsstudie 2006
Pilot results available	

Name of Indicator	**Best method of managing risks in the future**
Definition	Opinion with regard to the best method of managing risks in the future.
Notes	
Question wording	What would most help UK businesses manage their risks in the future? *(exact wording unavailable)* • Provision of more information security advice or information • More research of information security risk trends • Wider promotion of information security management standards • Development or promotion of technical security standards • More education for the general public about information security risks • More industry initiatives to address security risks • Nothing - there is enough being done at the moment
Source	DTI information **security** breaches survey 2006, technical report (enterprises)
Pilot results available	

It can be more secure to a computer room not only locking it, but also take some more protection towards the technical equipment.

Name of Indicator	**Physical security measures**
Definition	UK businesses that state in which way they protect their data centre or computer room, as share of businesses having one of these.
Notes	
Question wording	(How do UK) businesses with a data centre or computer room protect it? *(exact wording unavailable)* • Restrictions on access (e.g. locks) • Monitoring access (e.g. logs, CCTV) • Environmental and fire suppression controls
Source	DTI information **security** breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Providing components in different premises**
Definition	Businesses using different places for storing their information.
Notes	
Question wording	*(translation from German)* Does your house have in stock essential components of its information processing in different places? (Hält Ihr Haus wesentliche Komponenten seiner Informationsverarbeitung an verschiedenen Orten vor?) Answer categories: Remote archive, roboter systems, mirrored data, additional computers/cluster (Auslagerungsarchiv; Robotersysteme; gespiegelte Daten, zusätzliche Rechner/ Cluster • yes, in different fire compartment (ja, in einem getrennten Brandabschnitt) • yes, in a different building (in einem anderen Gebäude) • yes, at premises of cooperation partner (bei einem Kooperationspartner) • yes, at external provider (bei einem externen Anbieter) • no (nein)
Source	<kes>/Microsoft-Sicherheitsstudie 2006
Pilot results available	

Name of Indicator	**Method of precaution against disasters**
Definition	Method of precaution against disasters.
Notes	
Question wording	What precautions do UK businesses take against disasters? *(exact wording unavailable)* • Backups of critical data • Backups stored off-site • Disaster recovery plan • Disaster recovery plan tested in the last year
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Frequency of backing up critical data**
Definition	UK businesses that state the frequency of backing up their critical data.
Notes	
Question wording	How frequently do UK businesses back up their critical data? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Software protection against viruses and malicious software**
Definition	UK businesses that state what precautions they have in place to protect themselves against viruses and malicious software.
Notes	Multiple answers possible
Question wording	What precautions do UK businesses have in place to protect themselves against viruses and malicious software? *(exact wording unavailable)* • Anti-virus software • Anti-spyware software • Software that searches for probable virus activity
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Frequency of updating anti-virus defences**
Definition	UK businesses that state how often they update their anti-virus defences.
Notes	
Question wording	How quickly do UK businesses update their anti-virus defences? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Intrusion detection software**
Definition	UK businesses that state where they have implemented detection or prevention software.
Notes	
Question wording	Where have UK businesses implemented intrusion detection or prevention software? *(exact wording unavailable)* • At the Internet gateway • On servers • On desktops • Not implemented
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Web-site security solutions**
Definition	UK businesses that state how they protect their web-sites.
Notes	
Question wording	How do UK businesses protect their web-sites? *(exact wording unavailable)* • Firewall • Automatic failover to backup site • Intrusion detection software • Intrusion prevention software
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Wireless network security solutions**
Definition	UK businesses that state how they protect their wireless networks.
Notes	
Question wording	How do UK businesses protect their wireless networks? *(exact wording unavailable)* • Secure placement of access points • Name of the network (service set identifier or SSID) changed from default • Encrypted signals • Connection restricted to known computers only (through MAC filtering) • No controls
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Staff Internet access control**
Definition	UK businesses that state how they control their staff's usage, as share of businesses having access to the internet.
Notes	Multiple answers possible
Question wording	How do UK businesses with Internet access control their staff's usage? *(exact wording unavailable)* • Acceptable usage policy • Internet access restricted to some staff only • Block access to inappropriate web-sites • Log and monitor web access • Scan incoming e-mail/web downloads for viruses • Filter incoming e-mail for spam • Block or quarantine suspicious e-mail attachments • Scan web downloads for spyware • Staff able to send encrypted messages to main business partners
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Staff use of private systems with enterprise IT**
Definition	Businesses that state whether it is allowed to connect private systems to the businesses network and how it is checked or avoided.
Notes	Multiple answers possible
Question wording	*(translation from German)* a) Are staff allowed to connect the following privately owned or administerd systems to the enterprise's hardware or networks? (Ist es Mitarbeitern erlaubt, folgende privat beschafften oder administrierten Systeme mit Unternehmenshardware oder –netzen zu verbinden? b) How is this technically monitored, or, respectively, prevented? (Wie wird das technisch überwacht bzw. verhindert?) • Notebooks, PDAs etc.. (LAN/WLAN-access)(Notebooks, PDAs usw. (LAN/WLAN-Zugang)) • PDAs, Smartphones etc. (synchronisation with PCs) (PDAs, Smartphones usw. (Synchronisation mit PCs)) • Mobile memory (USB, firewire, digital cameras) (mobile Speicher (USB, Firewire, Digitalkameras, ...)) • networks hardware (switches, WLAN-Aps, modems) (Netzwerkhardware (Switches, WLAN-APs, Modems ...)) • Other peripherals (e.g. printers) (sonstige Peripherie (z. B. Drucker))
Source	<kes>/Microsoft-Sicherheitsstudie 2006
Pilot results available	

Name of Indicator	**E-mail scanning**
Definition	Type of scans UK businesses carry out on outgoing e-mail.
Notes	Multiple answers possible
Question wording	What scans do UK businesses carry out on outgoing e-mail? *(exact wording unavailable)* • Viruses, including Trojans • Confidential information • Inappropriate content • Unencrypted information that should be encrypted • No scans
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Removable media devices precautions**
Definition	Precautions they taken over removable media devices.
Notes	
Question wording	What precautions do UK businesses take over removable media devices? *(exact wording unavailable)* • Staff are told not to use such devices • Technical configuration of PCs prevents use • Confidential data is encrypted • No steps taken
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Instant messaging precautions**
Definition	Precautions with regard to instant messaging
Notes	
Question wording	What precautions do UK businesses that allow instant messaging (IM) take over its use? *(exact wording unavailable)* • Acceptable usage policy • Using a private and internally managed IM service • Scanning incoming messages for junk messages (spim) • Scanning outgoing messages for inappropriate content • Logging and auditing messages • Restricting which staff can use IM • No controls
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**IP telephony**
Definition	UK businesses that are implementing Voice over IP telephony.
Notes	
Question wording	(How many UK businesses are) implementing Voice over IP telephony? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Security expenditure**
Definition	UK businesses that state the change of security expenditure over the last year.
Notes	
Question wording	Has information security expenditure increased or decreased over the last year? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**IT budget spent on IT security**
Definition	UK businesses that state the percentage of IT budget spent on information security.
Notes	
Question wording	What percentage of IT budget was spent on information security, if any? *(exact wording unavailable)*
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Decision mechanism about spendings on information security**
Definition	Decision mechanism of UK businesses about spending on information security.
Notes	
Question wording	How do UK businesses decide what to spend on information security? *(exact wording unavailable)* • Formal business case • Quantify the benefits • Evaluate return on investment
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Drivers of information security expenditure.**
Definition	Drivers of information security expenditure.
Notes	Multiple answers possible
Question wording	What drives information security expenditure? *(exact wording unavailable)* • Protecting customer information • Maintaining data integrity • Protecting the organisation's reputation • Business continuity in a disaster situation • Complying with laws and regulations • Preventing downtime and outages • Protecting other assets (e.g. cash from theft) • Improving efficiency/cost reduction • Protecting intellectual property • Enabling business opportunities
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	
Definition	Procedures in place to respond to security incidents.
Notes	Multiple answers possible
Question wording	What procedures do UK businesses have in place to respond to security incidents? *(exact wording unavailable)* • Logging and responding to security incidents • Maintaining evidence to legal standard • Contingency plans for dealing with possible security breaches • Procedures for dealing with claims that an outsider has taken control of network • Specialist insurance policies covering damage suffered from cybercrime or viruses
Source	DTI information **security** breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Type of security incidents planed for**
Definition	Type of security incidents UK businesses plan for and how effective those are.
Notes	
Question wording	What type of security incidents do businesses plan for, and how effective are those contingency plans? *(exact wording unavailable)* • Infection by malicious software • Contingency plan in place and was effective • Staff misuse of Internet or e-mail • Infringement of laws or regulations • Attack on web-site or Internet gateway • Systems failure or data corruption • Fraud or theft involving computers • Theft or unauthorised disclosure of data • Physical theft of computer equipment
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Addressing the weaknesses that caused incident**
Definition	UK businesses that state how they addressed the weakness that caused their worst incident.
Notes	
Question wording	How did UK businesses address the weaknesses that caused their worst incident? *(exact wording unavailable)* • Additional staff training • Changes to policies and procedures • Changes to back up and contingency plans • Changes to configuration of existing systems • Deployment of additional security technology
Source	DTI information security breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Regular teaching of staff**
Definition	Businesses that teach or inform about IT security.
Notes	Multiple answers possible
Question wording	*(translation from German)* Whom does your house inform or teach about questions of information security (Wen informieren/schult Ihr Haus über Fragen der ISi?) Categories: frequently/regularly; occasionally/at special occasions; never; not answerable (häufig/regelmäßig (min 1x jährl.); gelegentlich / zu speziellen Anlässen; nie; n. b.) • Users (Benutzer) • Freelancers, external colleagues (freie/externe Mitarbeiter) • Data /information processing employees (IV-/DV-Mitarbeiter) • data protection commissioner (Datenschutzbeauftragte) • information security commissioner (ISi-Beauftragte) • Auditors (Revisoren, Prüfer) • Management • Others (andere)
Source	<kes>/Microsoft-Sicherheitsstudie 2006
Pilot results available	

Name of Indicator	**Teaching methods**
Definition	Teaching methods
Notes	Multiple answers possible
Question wording	*(translation from German)* What methods of teaching does your house preferanbly use in the area of information security? (Welche Ausbildungsmethoden setzt Ihr Haus auf dem Gebiet der ISi bevorzugt ein?) Categories: frequently; occasionally; never, not answerable (häufig; gelegentlich; nie; n. b.) • Internal instruction through teacher centred lectures, preferably enterprise-wide (interne Schulungen durch Frontalunterricht möglichst flächendeckend) • Internal instruction through teacher centred lectures, for special groups (interne Schulungen durch Frontalunterricht für Spezialgruppen • external instruciton (externe Schulungen(• Learning material for self learning (Materialien (Schulungsunterlagen) zum Selbstlernen) • Multimedia CD for self learning ((Multimediale) Lern-CDs zum Selbstlernen) • Online training applications/tools(Online-Trainings-Anwendungen/-Tools)
Source	<kes>/Microsoft-Sicherheitsstudie 2006
Pilot results available	

Miscellaneous: Security in outsourcing

Name of Indicator	**Outsourcing of IT operations**
Definition	Businesses having outsourced any of their IT operations.
Notes	
Question wording	(How many UK businesses have) outsourced any of their IT operations? *(exact wording unavailable)*
Source	DTI information **security** breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Number of outsource arrangements**
Definition	Number of outsource arrangements in businesses having Service Level Agreements in place, as share of businesses having outsourced any of its IT operations.
Notes	
Question wording	(How many UK businesses) outsource arrangements have Service Level Agreements in place? *(exact wording unavailable)*
Source	DTI information **security** breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Security of offshored IT activities**
Definition	UK businesses that state the way of making sure that offshored IT activities are secure, as share of businesses having offshored any of their IT operations.
Notes	
Question wording	How do UK businesses that have offshored IT activities ensure thay are secure? • Addressing data protection requirements in contract • Restricting which systems and data offshore personnel can access • Visiting offshore locations to check compliance with procedures • Independent audit by a third party (e.g. SAS 70 report) • No checks are performed
Source	DTI information **security** breaches survey 2006, technical report (enterprises)
Pilot results available	

Name of Indicator	**Outsourcing of functions**
Definition	Businesses having outsourced special functions.
Notes	
Question wording	(a) Does your house use outsourcing? (Betreibt Ihr Haus Outsourcing?) *(translation from German)* (b) if yes: which functions have you outsourced? (falls ja: Welche Funktionen haben Sie ausgelagert?) • external information security agent (externer ISi-Beauftragter) • entire computer centre/ IT (gesamte(s) Rechenzentrum/IT) • Surveillance, monitoring, quality control (Überwachung, Kontrolle, Qualitätssicherung) • emergency provisions / business continuity (Notfallvorsorge/Business Continuity) • Managed Firewall/IDS/IPS (ditto) • application systems (Anwendungssysteme) • content security / virus blocking (Content Security/Virenabwehr) • data bank systems, tools (Datenbank-Systeme, Werkzeuge) • network management (Netzwerk-Management) • building services (Haustechnik) • data backup solutions (Datensicherung, Backup-Lösungen) • data protection (Datenschutz) • documentation, archiving (Dokumentation, Archivierung) • destruciton of data carriers (paper, IT) (Vernichtung von Datenträgern (Papier, EDV)) • personnel deployment, HR (Personaleinsatz, Personalentwicklung, Mitarbeiterweiterbildung) • OS maintenance, administration (Betriebssystempflege/Administration) • other (please specify) (Sonstiges (bitte nennen)) (c) if yes: do you have service level agreements/ contractual agreements with the outsourcing party (*sic)*? (falls ja: Haben Sie Service-Level-Agreements/ vertragliche Vereinbarungen mit dem Outsourcer? • yes, involving regular monitoring / yes, including occasion based monitoring / yes but without monitoring / no (ja, mit regelmäßiger Kontrolle; ja, mit anlassbezogener Kontrolle; ja, aber keine Kontrolle; nein) • including explicit information security requirements? (mit expliziten Anforderungen an die ISi?) • including explicit data protection requirements? (mit expliziten Anforderungen an den Datenschutz?) (d) Are you content about outsourcing? (Sind Sie mit dem Outsourcing zufrieden?) • yes, absolutely (ja, uneingeschränkt) • yes, with reservations (ja, mit Einschränkungen) • no (nein) • not answerable (nicht beantwortbar)
Source	<kes>/Microsoft-Sicherheitsstudie 2006
Pilot results available	